AMENDMENT TO THE CLAIMS

1. (Currently Amended) A computer-implemented method for enhancing the security of informational interactions with a biometric device, comprising:

pre-establishing an encryption relationship between a computing device and the biometric device, wherein the computing device and biometric device include separate but related encryption components and the biometric device encryption component is implemented as firmware and decrypts information encrypted by the computing device encryption component;

generating a session packet, wherein generating a session packet comprises generating a session number, generating a session time stamp, obtaining a session key, and storing ~~it~~ the session number, the session time stamp, and the session key in the session packet;

maintaining a record of the session number, the session time stamp, and the session key in a database associated with the computing device;

encrypting the session packet utilizing the computing device encryption component and transmitting it to the biometric device;

receiving a biometric information packet from the biometric device, decrypting it with an encryption key that is complimentarily related to the session key, and making a determination as to whether or not to utilize a collection of biometric data contained in the decrypted biometric information packet, wherein making a

determination comprises comparing a session number received with or as part of the biometric information packet to the record of the session number and evaluating the session time stamp to determine whether the biometric information packet was received within a predetermined time period; and

wherein pre-establishing, generating, maintaining, encrypting, and receiving enhance the security of informational interactions between the biometric device that collects the collection of biometric data and the computing device that selectively utilizes the collection of biometric data.

2. (Previously Presented) The method of claim 1, wherein the method is performed in the consecutive order of pre-establishing, generating, maintaining, encrypting, and receiving.

3-6. (Cancelled)

7. (Currently Amended) The method of claim ~~4~~ 1, wherein obtaining a session key comprises generating a public key portion of a PKI key pair.

8. (Original) The method of claim 7, wherein receiving a biometric information packet and decrypting it comprises receiving a biometric information packet and decrypting it with a private key portion of the PKI key pair.

9-14. (Cancelled)

15. (Previously Presented) The method of claim 1, wherein making a determination further comprises comparing a data representation of a user's biometric information to at least one data representation of biometric information stored in a database.

16-18. (Cancelled)

19.(Original) The method of claim 1, wherein pre-establishing an encryption relationship comprises storing a first part of a PKI key pair with the computing device and a second part of the PKI key pair with the biometric device.

20. (Previously Presented) The method of claim 19, wherein encrypting the session packet comprises encrypting the session packet utilizing the first part of the PKI key pair.

21.(Previously Presented) The method of claim 1, wherein pre-establishing an encryption relationship comprises storing a first part of a static encryption key pair with the computing device and a second part of the static encryption key pair with the biometric device, one of the first and second parts being configured to decrypt information that has previously been encrypted utilizing the other part.

22. (Previously Presented) The method of claim 21, wherein encrypting the session packet comprises encrypting the session packet utilizing the first part of the static encryption key pair.

23-51. (Cancelled)

52. (New) A biometric security system comprising:

a computing device having a first encryption component, a first encryption program, a processor, and a first interface, wherein the computing devices generates a session packet that is encrypted using the first encryption component and wherein the session packet comprises a session number, a session key, a command, a time stamp, and a first set of data;

a database associated with the computing device, wherein the database stores a record of the session number, the session key, and the time stamp;

a reader having a second encryption component, a second encryption program, and a second interface, wherein the reader generates a biometric information packet based upon the command, wherein the biometric information packet is encrypted using the session key, and wherein the biometric information packet comprises the session number, a model, and a second set of data;

wherein the session packet is transmitted from the first interface to the second interface and the reader decrypts the session packet with the second encryption component;

wherein the biometric information packet is transmitted from the second interface to the first interface and the computing device decrypts

the biometric information packet with an encryption key that is complimentarily related to the session key;

wherein the second encryption component is implemented as firmware and decrypts information encrypted by the first encryption component; and

wherein the processor selectively utilizes the model based upon a comparison of the session number to a copy of the session number retrieved from the database and a comparison of the time stamp to a time indicative of when the biometric information packet was received by the computing device.

53. (New) The biometric security system of claim 52 wherein the computing device generates the session packet in response to a request from the reader.

54. (New) The biometric security system of claim 52 wherein the computing device generates the session packet in response to a request from an independent application associated with the reader.

55. (New) The biometric security system of claim 52 wherein the computing device generates the session packet in response to a request for secured rights.

56. (New) The biometric security system of claim 52 wherein the session key is a public key and the encryption key complimentarily related to the session key is a private key.

57. (New) The biometric security system of claim 52 wherein the first encryption component is a first part of a PKI key pair and the second encryption component is a second part of the PKI key pair.

58. (New) The biometric security system of claim 52 wherein the first encryption component is a first part of a static key pair and the second encryption component is a second part of a static key pair.

59. (New) The biometric security system of claim 52 wherein the model comprises a collection of biometric information.

60. (New) The biometric security system of claim 59 wherein the collection of biometric information is collected as part of an enrollment operation and wherein the processor selectively utilizes the model by storing a copy of the model in the database.

61. (New) The biometric security system of claim 59 wherein the collection of biometric information is collected as part of an authorization operation and wherein the processor selectively utilizes the model to grant an access right.

62. (New) The biometric security system of claim 61 wherein the processor selectively utilizes the model to grant an access right comprises a comparison of the model to a match template stored in the database.

63. (New) The biometric security system of claim 52 wherein the processor performs an image qualification function on at least part of a collection of available image data and wherein the image qualification comprises determining whether the collection of available image data is fraudulent.

64. (New) The biometric security system of claim 52 wherein the processor performs an image qualification function on at least part of a collection of available image data and wherein the image qualification comprises determining whether the collection of available image data is of sufficient quality.

65. (New) The biometric security system of claim 52 wherein the processor performs an image qualification function on at least part of a collection of available image data and wherein the image qualification comprises determining whether the collection of available image data is fraudulent and whether the collection of available image data is of sufficient quality.

66. (New) A computer-implement method for enhancing the security of informational interactions with a biometric device, the method comprising:

pre-establishing an encryption relationship between the biometric device and a computing device, wherein pre-establishing comprises storing a first encryption component in the biometric device that is directly affiliated to a second encryption component stored in the computing device;

requesting an access right associated with the computing device;

initiating an authorization session;

generating a session packet that includes a unique session number and a public key portion of a PKI key pair;

retaining a copy of the session number and a private key portion of the PKI key pair;

encrypting the session packet utilizing the second encryption component;

transmitting the encrypted session packet that includes the session number and the public key portion of the PKI key pair to the biometric device;

decrypting the session packet utilizing the first encryption component;

collecting a set of biometric information from a system operator;

generating a biometric information packet that includes the set of biometric information and the session number;

encrypting the biometric information packet utilizing the public key portion of the PKI key pair that was transmitted to the biometric device in the encrypted session packet;

transmitting the encrypted biometric information packet to the computing device;

decrypting the encrypted biometric information packet utilizing the retained private key portion of the PKI key pair;

comparing the retained copy of the session number to the session number included in the biometric packet;

comparing a time frame to a predetermined time frame, wherein the time frame is based at least partially upon the time that the encrypted biometric packet is received by the computing device;

utilizing the set of biometric information based upon a determination that the retained copy of the session number matches the session number included in the biometric packet and based upon a determination that the time frame is within the predetermined time frame;

not utilizing the set of biometric information based upon a determination that the retained copy of the session number does not match the session number included in the biometric packet; and

not utilizing the set of biometric information based upon a determination that the time frame is not within the predetermined time frame.

67. (New) The computer-implemented method of claim 66 wherein utilizing the set of biometric data comprises transferring the set of biometric information to a processor associated with the computing device.

68. (New) The computer-implemented method of claim 67 wherein transferring the biometric information to the processor associated with the computing device comprises transferring the biometric information to the processor for processing.

69. (New) The computer-implemented method of claim 68 wherein processing comprises an authentication.

70. (New) The computer-implemented method of claim 68 wherein processing comprises an enrollment.

71. (New) The computer-implemented method of claim 66 wherein the authorization session opens upon initiation and closes after a predetermined time.

72. (New) The computer-implemented method of claim 71 wherein the predetermined time comprises the amount of time required for the biometric device to complete a scan.

73. (New) The computer-implemented method of claim 66 wherein the unique session number comprises a non-consecutive number that is unique to a particular session.

74. (New) The computer-implemented method of claim 66 wherein the public key is unique to a particular session.

75. (New) The computer-implemented method of claim 66 wherein the public key is the same for multiple sessions.

76. (New) The computer-implemented method of claim 66 wherein collecting a set of biometric information from a system operator is based on a command received in the session packet.

77. (New) The computer-implemented method of claim 66 wherein the first encryption component is implemented as firmware.

78. (New) The computer-implemented method of claim 66 wherein the first encryption component is implemented as flash memory.